Overview of Akamai's Personal Data Processing Activities and Roles in connection with Services Provisioning

Last Updated: August 2021

This document is maintained by the Akamai Global Data Protection Office

Table of Contents

Introduction

Akamai Technologies, Inc. and its operated global affiliates ("Akamai") is a global leader in content delivery and security services designed to make the Internet fast, reliable and secure for its customers. Akamai operates over 350,000 servers, in over 1,600 networks within more than 130 countries (the "Akamai Edge"). Akamai follows a data protection and privacy framework designed to comply with data protection obligations around the globe and takes its obligations under applicable data protection laws very seriously.

This document provides an overview of Akamai's personal data processing activities associated with the Services it provides to customers.

Some Useful Terms

"**Akamai Services**", "**Services"** means services or products as described in the Akamai services page which may be ordered by the Customer.

"Customer" means an entity purchasing Akamai Services directly or indirectly via an Akamai partner.

"**Customer Content**" means all Web Properties and applications, including any third-party content or applications, provided to Akamai in connection with a Customer's access to or use of the Akamai Services.

"**Data Protection Laws**" means all applicable laws (including decisions and guidance by relevant supervisory authorities) relating to data protection, the processing of personal data or personal information, and privacy applicable to Akamai and the Customer with respect to the processing of Personal Data to provide the Akamai Services, including such laws, by way of example and without limitation, the General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA"), the Brazilian General Data Protection Law ("LGPD") and the Personal Information Protection and Electronic Documents Act ("PIPEDA").

"**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws, and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., "Business" instead of "Data Controller" and "Service Provider" instead of "Data Processor" under the CCPA, or "organization" or "agency" under the Australian Privacy Principles, "Data Operator" instead of "Data Processor" under LGPD).

"End User" means the natural person that accesses Customer Content or otherwise uses a Customer's services on the Internet.

"**Session**" or "**Web Session**" means a single visit by an End User or automated client to particular Customer Content or other location on the Internet.

"**Web Property**" means a point of presence (e.g., a website, social media site or account, blog, etc.) on the Internet that is an asset of an entity (e.g. an individual or corporation) used for the purpose of representing a brand, person or other identity.

Personal Data Processing related to Akamai Services Provisioning

Figure 1: Akamai's Role depending on data category

Data subject	Category of Personal Data	Akamai's Role
Customer/ prospective Customer or their representative	Contact Information	Controller
Partner/ prospective partner or their representative	Contact Information	Controller
End User accessing Akamai's Customers' websites or applications	End User Personal Data	Processor
	Logged Personal Data	Controller and Processor
	Site Personal Data	Processor
	Enterprise Personal Data	Processor

Categories of Personal Data

In providing the various Services to its Customers, Akamai processes the following categories of data:

1) With respect to Customers and partners and their representatives:

(i) **Contact Information**: Personal Data of Customer's or partner's employees and representatives collected and maintained by Akamai to support the customer relationship ("Contact Information"). Contact Information may include, by way of example only, such data as:

a. Contact names

b. Title

c. Business addresses

d. Email addresses

e. Telephone numbers

f. Akamai's customer portals or API credentials

2) With respect to End Users accessing Akamai's Customers' websites or applications:

(i) **End User Personal Data**: Akamai processes Personal Data included within Customer Content ("End User Personal Data") when providing Services to its Customers. The Customer determines what data will be included in End User Personal Data. As examples, End User Personal Data may include data such as:

a. Login credentials

b. Subscriber name and contact information

c. Financial or other transaction information

d. Other Personal Data relating to the individual data subject as set by the Customer

(ii) **Logged Personal Data:** Akamai processes Personal Data that is included in log files when performing Services for Customers ("Logged Personal Data"). Logged Personal Data is Personal Data logged by Akamai servers, relating to the access by End Users to Customer Content via the Akamai Edge, as well as logged personal data associated with End User activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's Session with the Customer's Web Property. Logged Personal Data include such data as:

a. End User IP addresses

b. URLs of sites visited with time stamps (with an associated IP address)

c. Geographic location based upon IP address and location of Akamai server

d. Telemetry data (e.g. mouse clicks, movement rates, and related browser data)

(iii) **Site Personal Data:** Akamai processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of a data subject's Session with the Customer's Web Property ("Site Personal Data"). The Site Personal Data consists of End User telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance. Akamai may also collect information from data analytics, including page activity data and URLs of websites visited, and location data of the edge server deployed closest to the End User that answered the access request made by the End User when accessing the websites and applications properties of Akamai's Customer.

(iv) **Enterprise Security Personal Data:** Akamai processes Personal Data on behalf of Customers of Akamai Enterprise Security Services that are provided by Customer or collected during the provision of Services in order to protect End Users of the Customer's enterprise network and the network itself from Internet security and

policy abuse risks ("Enterprise Security Personal Data"). The Enterprise Security Personal Data includes such data as:

a. Login and user authentication data

b. Contents of communications, including attachments

c. Browser and device information (like MAC address or IP address) including location information

d. URLs visited

Akamai's Policy Towards IP Addresses

Akamai treats IP addresses generally as Personal Data under the Data Protection Laws because, when processed for the purpose of identification of an individual, IP addresses can be combined with other data and used to identify an individual that was assigned that particular IP address during one or more Sessions.

In a large number of cases the IP addresses processed by Akamai will not be assigned to any individual, but rather will identify only the latest server from which a given IP data packet was sent. Only if the processing party can demonstrate that a given IP address is not associated with an individual (such as IP addresses associated with a corporate firewall), however, should such IP addresses be treated as non-personal data.

In many cases, the primary piece of Personal Data that Akamai processes and collects will be the IP address associated with a given web or IP Session. Indeed, many data elements identified by Akamai as Personal Data, such as Universal Resource Locators or URLs (e.g. http://www.akamai.com), are only Personal Data when combined with an associated End User IP address. Akamai systems are not designed, however, to differentiate between an IP address that may be an individual's IP address and one that is not (i.e. an IP address of a server or router in the delivery chain of the session) and, therefore, as a matter of internal policy, all IP addresses at Akamai are treated as Personal Data.

The above policy notwithstanding, it is important to note that while Akamai collects and processes IP addresses as described above, it does not do so in a manner that gives Akamai the ability to identify any given individual associated with a web transaction. As an essential part of making sure End Users can securely access the websites and applications pages and content they request, Akamai must handle certain data, including end user IP addresses, but Akamai does not identify the end user using an IP address when doing so. Rather, Akamai's processing of IP addresses is conducted to provide the contracted services and identify events and activities between computers and agents (such as browsers) on the Internet (e.g. determining whether an action on a website is being performed by a human or a bot) or other identify patterns that may indicate malicious or fraudulent activity.

General Principles in Data Processing

Akamai processes Personal Data in compliance with the principles set forth in the applicable Data Protection Laws. Akamai processes only the Personal Data necessary and proportionate to meet the purposes outlined herein, and does so in a fair and lawful manner taking into consideration not only our obligations to our Customers but the potential impacts and risks to individual Data Subjects posed by our data processing activities. Akamai takes steps to mitigate such impacts and risks and to secure the data in our possession. As discussed above, the processing of Personal Data conducted by Akamai is not used by Akamai to identify any individuals, but rather to identify events and activities between computers and agents (e.g. browsers) on the Internet, such as determining whether an action on a website is being performed by a human or a bot.

While Akamai remains responsible for the processing of Personal Data as outlined herein, for certain Services we may use third party service providers as listed in Akamai's sub-processor list.

Description of Processing by Category

Contact Information

Akamai collects and processes Contact Information to provide access to and use of tools to support the Services, communications with customers, and to manage customer relations. This data is stored by Akamai in its portal(s) (such as Akamai Control Center), customer community and developer sites, and in internal business process tools.

Retention period: Data will be retained as long as required for the customer relationship.

End User Personal Data

Akamai operates largely as a conduit for End User Personal Data transmitted by its Customers via the Akamai Edge. The Customer determines: what End User Personal Data is processed by its Web Property, whether to use secure services offered by Akamai for encrypted delivery of Customer Content and whether or not any Customer Content is cached by Akamai's servers. Akamai determines how to optimally route and secure such End User Personal Data via the Akamai Edge based upon numerous factors including customer configurations, applied security rules, Internet congestion, and best available routes.

As described above, Customer determines through design and configuration of its Web Properties and Customer Content and instructions entered via Akamai's service portals (e.g. Akamai Control Center), what End User Personal Data will flow across the Akamai Edge. The Customer, therefore, will be responsible for compliance with applicable laws for such processing (e.g. appropriate end user notices or a legal basis for processing End User

Personal Data, and having chosen services appropriate for the type of End User Personal Data transiting Akamai's servers (e.g. PCI compliant services and encryption settings)).

Absent Customer instructions, Akamai does not process End User Personal Data other than as required to provide the Services purchased by the Customer.

Retention period: Akamai recommends configuring the services to have End User Personal Data transmit the Akamai edge servers and to not store/cache such Data. Such data will be stored/cached only if instructed so by Akamai's Customer and retained in accordance with the Customer's instructions.

Logged Personal Data

Akamai conducts analysis of traffic traversing its network both from system logs and data collected from the Web Session or an End User's browser, which sometimes includes Personal Data, in order to deliver and improve its Services, and provide Customers with data analytics products related to performance of the Services and the Customer Content, as well as provide fraud and bot management capabilities. Akamai also conducts traffic analysis to derive and compile information relating to the type, nature, content, identity, behavior, signature, source, frequency, reputation and other characteristics of malicious Internet traffic and activity. The resulting threat data is integrated into Akamai's tools, products (including data products that contain a subset of the threat data, which are sold to the Akamai's customers as part of its security service offerings), and services to protect itself and its customers from cyber-attacks, hacking, malware, viruses, fraud, exploits and other malicious activity.

Logged Personal Data may also be processed for purposes of billing, service issue resolution and service improvement (e.g. mapping decisions) and aggregate reporting (aggregate reports do not identify any Customer or the Data Subjects visiting their web properties) such as Akamai's "State of the Internet" report.

Retention period: Data will be retained for up to 90 days in most of the cases. Where specific security events require updates of the existing algorithm, such data is retained for up to 180 days.

Site Personal Data

Akamai processes Site Personal Data to provide website monitoring and analytics services to Customers to enable them to understand the nature of End User traffic to their Customer Content, as well as to monitor the performance of such properties.

Retention period: Data will be retained on the local edge server in accordance with the load of the edge server, usually a couple of hours.

Enterprise Security Personal Data

Akamai's Enterprise Security Services provide Customers with tools and services to protect their employees and guests, as well as their network infrastructure from Internet threats. In addition, these same tools may be used to monitor network activity, provide secure access to applications and network resources, and establish and enforce access policies. To provide these Services, Akamai processes Enterprise Security Personal Data as needed to control access and monitor network traffic, processes and may store access credentials and related network data.

Retention period: Data will be retained for 90 days except for data necessary for operation of the Services, which will be retained only as long as needed for the service relationship.

Akamai's Operates Both as a Data Controller and a Data Processor

In reviewing any processing of Personal Data under Data Protection Laws and similar laws, it is critical to understand the relative processing roles and which role each player assumes. In any given data processing scenario between multiple parties, parties may each be Data Processors or Data Controllers or both in their own rights. In order to understand the differing obligations of the parties and particularly to recognize when the more strict obligations of the Data Controller must be applied, we must properly designate these roles based upon the factual analysis of the various data processing activities.[1]

Traditionally, parties to a commercial agreement have simply designated any service provider as a Data Processor, the ordering entity as the Data Controller and taken the analysis no further. According to the EU Advocate General, however, "[a]ny interpretation that is based solely on the terms and conditions of the contract concluded by the [parties should] be rejected."[2] The division of tasks in a contract can only suggest the actual roles of the parties, for "[i]f it were otherwise, the parties would be able artificially to assign responsibility for the data processing to one or other of themselves."[3] Ever more frequently data processing is complex, comprising many distinct processes which involve numerous parties with differing degrees of control. Thus the traditional role is no longer automatically valid.

A Data Controller "alone or jointly with others, determines the **purposes** and **means** of the processing of personal data." This role is in contrast to the Data Processor role where the person or entity merely "processes personal data **on behalf of** the controller", subject to the authorization and explicit instruction of the Data Controller.

[1] "The concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis'. See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 21.
[2] Opinion of Advocate General BOT delivered 24 October 2017, Case C-210/16, p. 60.
[3] *Id.*

Akamai's activities as described above make it:

(i) **Data Processor** with respect to End User Personal Data, Logged Personal Data processed in the course of performing the Services, Site Personal Data, Enterprise Security Personal Data.

Akamai does not collect these data elements for its own purposes but processes these data elements as a "Data Processor" or "Service Provider" (i.e., on behalf of our Customers, subject to their instruction) assisting the Customer by making the Customer Content available to the Customer's End Users in a fast, reliable and secure manner.

For this data Akamai's Customer determines the data elements processed. Customer then purchases Akamai Services, and determines the Service configuration (e.g. the data elements to be cached and the time to cache, the data elements not to be cached) made available by Akamai via its service portal(s) and finally it makes choices regarding security and encryption options offered by Akamai. By controlling the Service configuration, the Customer is providing the data processing instructions to Akamai[4].

In the above scenario, Akamai has no control over or visibility into the specific data elements that transit its servers. Such control and visibility is maintained by the Customer. Akamai's role is restricted to offer the above listed configuration choices as non-essential means to best accommodate the Customer's interest to process the End User Personal Data, Logged Personal Data, Site Personal data and Enterprise Security Personal Data[5]. In addition, Akamai operates largely as a conduit for End User Personal Data collected, processed, and transmitted by its Customers via Akamai services. The Customer determines what End User Personal Data is collected or otherwise used and how it will be processed by Akamai. The Customer, therefore, is responsible for compliance with applicable laws for such processing (e.g., appropriate end-user notices or consents and having chosen services appropriate for the type of End User Personal Data transiting Akamai's servers).

Akamai and Customer agree on a data processing and/or data transfer agreement to contractually ensure that Customer is responsible for the data processing activities, while Akamai follows the instructions provided by the Customer and has in place appropriate technical and organisational measures to secure the data processed by Akamai. In addition Akamai assists the Customer to understand the data flows and privacy risks related to the Akamai Services via workshops and documentation. This

[4] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 40.

[5] "When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller." see the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 28.

enables the Customer as Data Controller to assess the risks and actively approve the way the processing is carried out [6].

In case of questions about Akamai's processing of Personal Data as Data Processor and execution of related data subject access rights, End Users should contact Akamai Customers directly.

(ii) **Data Controller** with respect to Logged Personal Data processed outside of direct Service performance and Contact Information.

Akamai processes Logged Personal Data outside of the direct performance of the Services for purposes of traffic analytics, monitoring and management of the Akamai systems, security analytics, service development, billing and internal reporting. Contact Information of Customer employees is processed by Akamai to manage the customer relationship.

Such purposes are determined by Akamai, as well as the data elements collected, processing systems and location, retention periods and security measures in place. The Customers do not participate in such determinations, they are not at all involved in these data processing activities. The Logged Personal Data and the Contact Information are collected independently by Akamai and it is solely Akamai determining the why, what and how of these processing activities[7].

As outlined above, Akamai complies with data protection requirements applicable to a Data Controller when processing such data, e.g. the privacy principles, security and notification obligations.

In case of questions about Akamai's processing of Personal Data as Data Controller and execution of related data subject access rights, data subjects shall contact Akamai directly as set forth in the Akamai Privacy Statement.

International Transfers of Personal Data

The Akamai Edge is designed in a manner that routes traffic through the best available routes regardless of geographic boundaries. The way the Akamai Edge operates is that the Customer Content will always be delivered by the optimally Akamai server (which will usually be the server that is physically closest to the End User). This means that when Customer Content is accessed by e.g. an End User located in the European Economic Area ("EEA"), in general the Customer Content and the embedded End User Personal Data will be transmitted via Akamai servers deployed in the EEA and there is no transfer of the End User Personal Data to servers deployed outside the EAA, however, in some cases (e.g. internet congestion or BGP routing issues) traffic delivery may occur from servers located outside of

[6] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 30 and 41.
[7] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 35.

the EEA, even if the End User requesting such data is located inside the EEA. In addition, certain systems Akamai operates are located in the USA (e.g. Akamai's security analytic systems and support ticket systems) and, therefore, certain data elements (e.g. Logged Personal Data) will be transferred to and processed in the USA.

To ensure 24/7 availability of the Services, Logged Personal Data is, for purposes of service issue resolution and system monitoring and maintenance, remotely accessed and processed by Akamai's support teams in the EU, UK, the USA and India.

For any international transfer within the Akamai group or to third party service providers, Akamai shall ensure that such recipients maintain appropriate contractual, technical and organisational safeguards and shall have in place required data protection terms to ensure protection of Personal Data to the same degree as required by Akamai and applicable Data Protection Laws (e.g. adequacy decision or Standard Contractual Clauses).

For details on international transfer and applicable safeguards please refer to the "Data Transfer by Akamai" section in the Akamai Privacy Trust Center and to Akamai's sub - processor list.

Additional information

Additional information regarding the data processed by Akamai as a Data Controller is published in the Akamai Privacy Statement to notify interested parties in a fair and transparent manner.

The data processing and data transfer agreement offered by Akamai to its Customers and Akamai's technical and organizational measures to secure the personal data processed as a Data Processor, are published in the Akamai Privacy Trust Center under the respective sections.